REMARKS

Claims 1-9, 11-14, 15-32, 34 and 35 have been rejected by the Examiner. No claim has been amended. Reconsideration of the application is respectfully requested.

CLAIM REJECTIONS UNDER 35 U.S.C. § 112

In "Claim Rejections – 35 USC § 112" on page 2 of the above-identified Office Action, claims 1 and 27 have been rejected under 35 USC § 112, para 1. In particular, the Examiner stated that claims 1 and 27 are not enabled since it is unclear how "receiving network traffic from the second device corresponding to a previous secure communication session established when the second device was previously on the internal network" can take place when the second device moves to the external network.

Applicants submit that such feature of claims 1 and 27 are fully enabled as recited in paragraph [0038] of the instant specification that a mobile control point (which may be deemed as the second device) having a previously established secured communciation session with a device (which may be deemed as the first device) on the internal network may have a new attachment to the external network. The traffic of this previously established communication session will route to the gateway of the internal network, and the gateway would force the control point to reestablish a communication session. So, Applicants submit that claims 1 and 27 are enabled based on such description and are patentable under 35 USC § 112, para 1.

CLAIM REJECTIONS UNDER 35 U.S.C. § 103

1. In "Claim Rejections – 35 USC § 103" item 3 on page 4 of the above-identified Office Action, claims 1-7, 9, 11 , 23-25, and 27-31 have been rejected as being unpatentable over U.S. Patent Application Publication No. 2003/0217136 (hereinafter Cho), in view of U.S. Patent Application Publication No. 2002/0103898 (hereinafter Moyer) under 35 U.S.C. § 103(a).

Independent claim 1 recites a method for an intermediary selectively coupling an external network and an internal network to dynamically generate filter rules to facilitate establishing an end to end secure session connection between a first device on the internal network and a second device of the external network, the method comprising:

> "receiving a secure session establishment request by the second device on the external network to establish a secure communication session with the first device on the internal network;
> forwarding the secure session establishment request to the first device;
> monitoring the internal network to detect an approval or disapproval acknowledgement by the first device for the secure session establishment request; and
> configuring a first filter rule of the intermediary to allow communication between the first and second devices through the intermediary, if an approval authentication acknowledgement is detected;
> receiving network traffic from the second device corresponding to a previous secure communication session established when the second device was previously on the internal network; and
> responding to said network traffic with an error such that the second device attempts to re-establish a secure communication session from the external network."

The Examiner cited paragraphs [0005]-[0006] of Cho to read on the two underlined elements of claim 1. In particular, the Examiner stated that Cho disclosed that a control point which receives messages while on the home network may travel outside the home network, and the control point may be a wireless client. Thus, the Examiner concluded that the control point in Cho may still be sending traffic belonging to a previous session to the home network as it travels beyond the range of the home network and cause an error condition to be generated, so that can be used to read on the second device in claim 1.

However, Applicants respectfully diagree. According to paragraph [0026], Cho discloses a proxy system for a home gateway designed to allow a user to control UPnP devices in a home network over an external Internet network using a wired/wireless Internet client. In particular, the cited paragraphs of Cho only disclose that a user could input control commands via user interface (UI) and UPnP application program interface (API), and a control point controls the specific device in response to the commands. And since the UPnP API and control point are all present in one system, it is hard for the user to control devices from outside of the home network. Nothing in Cho teaches or suggests that the control point may move outside the home network. It is actually the user that can move beyond the home network and control the UPnP devices with a internet client program, while the control point in Cho should be still attached to the system in order to operate the device on the home network. So, Applicants submit that Cho fails to identify a second device on the external network as recited in claim 1.

Notwithstanding the above, Applicants submit that Cho does not disclose the intermediary in claim 1 that is configured to receive network traffic from the second device corresponding to a previous secure communication session established when the second device was previously on the internal network, and respond to said network traffic with an error such that the second device attempts to re-establish a secure communication session from the external network, as recited in claim 1. In the Office Action, the Examiner read the UPnP proxy server in Cho as the intermediary in claim 1. However, Applicants repectfully diagree.

The UPnP proxy server in Cho includes an agent for receiving commands from the internet clients, and a bridge for sending control messages to the UPnP devices on the home network. Figures 3 of Cho is the operating flowchart of the agent and Figure 5 of Cho is the operating flow chart of the bridge. As illustrated in Figure 3 of Cho, the agent only determines that if the message is a web page request message or a device control message. As illustrated in Figure 5 of Cho, the bridge only determines that if the message is from the agent or from the UPnP device, and if the message is a device control command or a event registration message. None of the figures disclose that the agent or the bridge of the UPnP proxy in Cho would determine as in claim 1 that if the messages belong to a communication session between the UPnP device on the home network and another device that roamed out from the home network.

Moyer is cited to read on the filter rules in claim 1. However, Moyer fails to cure the deficiency of Cho. Therefore, the combination of Cho and Moyer fails to teach or suggest each and every element of claim 1.

Further, Applicants submit that there would have been no motivation to modify Cho to achieve what is recited in claim 1. According to paragraph [0006] of Cho, the purpose of Cho is to control and manage UPnP devices in the home network over an external internet network. Incorporating elements in claim 1 which are directed to establish sercure UPnP communication sessions between devices located on different networks, would have no contribution to the purpose of Cho. Therefore, Applicants submit that there would have been no motivation to modify Cho to achieve claim 1.

Claims 23 and 27 recite in general similar subject matter to claim 1. Claims 2-7, 9, 11, 24-25, and 28-31 depend from claims 1, 23 or 27 respectively, incorporating their recitations. Therefore, due to at least above stated reasons, claims 2-7, 9, 11, 23-25, and 27-31 are patentable over the combination of Cho and Moyer under 35 U.S.C. § 103(a).

2. In "Claim Rejections – 35 USC § 103" on page 12 of the above-identified Office Action, claims 12-14, 16-20, 22, 32, and 34-35 were rejected as being unpatentable over Cho, IETF draft "Simple Service Discovery Protocol/1.0" (hereinafter IETF-Draft-SSDP), and Moyer under 35 U.S.C. § 103(a).

Independent claim 12 recites

> "a method for a second device communicating with a first device on the internal network by way of an intermediary selectively coupling an external network and the internal network, comprising:
>
> receiving, by the second device while on the internal network, a presence advertisement for the first device;
>
> storing, by the second device while on the internal network, a network address associated with the first device;
>
> determining, by the second device while on the internal network, services offered by the first device; and
>
> issuing, by the second device while on the external network, a secure communication initiation request to the first device via the intermediary."

Thus, read as a whole, claim 12 recites a method for a second device which moves between the internal and external networks to communicate with a first device on the internal network via an intermediary.

As stated section 1, Cho and Moyer fail to disclose such a second device as similarly recited in claim 1. IETF-Draft-SSDP is cited to read on "determining, by the second device while on the internal network, services offered by the first device" as recited in claim 12. However, IETF-Draft-SSDP fails to cure the deficiency of Cho and Moyer.

Therefore, due to at least on of the reasons stated in section 1, Applicants submit that the combination of Cho, Moyer and IETF-Draft-SSDP fails to teach or suggest each and every element of claim 12 and claim 12 is patentable over Cho, Moyer and IETF-Draft-SSDP under 35 U.S.C. § 103(a).

Claim 32 recites in general similar subject matter to claim 12. Claims 13-14, 16-20, 22, and 34-35 depend from claim 12 or 32 respectively, incorporating their recitations. Therefore, at least due to above discussed reasons, claims 13-14, 16-20, 22, 32, and 34-35 are patentable over Cho, Moyer and IETF-Draft-SSDP under 35 U.S.C. § 103(a).

3. In "Claim Rejections – 35 USC § 103" on page 18 of the above-identified Office Action, claim 8 was rejected as being unpatentable over Cho, Moyer and in view of U.S. Patent Application Publication No. 2005/0111382 (hereinafter Le) under 35 U.S.C. § 103(a).

Claim 8 depends from amended claim 1, incorporating its recitations. Le is cited to read on communication within the internal network is accord with an IPv6 compatible Internet protocol in claim 8. However, Le fails to cure the deficiency of Cho and Moyer. Therefore, due to at least one of the reasons above in section 1, claim 8 is patentable over Cho, Moyer and Le under 35 U.S.C. § 103(a).

4. In "Claim Rejections – 35 USC § 103" on page 19 of the above-identified Office Action, claim 21 was rejected as being unpatentable over Cho, IETF-Draft-SSDP, Moyer and IETF RFC 3056, "Connection of IPv6 domains via IPv4 clouds" (hereinafter RFC 3056) under 35 U.S.C. § 103(a).

Claim 21 depends from claim 12, incorporating its recitations. RFC 3056 is cited to read on using the prefix of a globally unique IPv6 address to identify an intermediary that connects an IPv6 cloud to the IPv4 network in claim 21. However, RFC 3056 fails to cure the above stated deficiency of Cho, IETF-Draft-SSDP and Moyer. So, based on at least one of the reasons stated above in section 1, claim 21 is patentable over Cho, IETF-Draft-SSDP, Moyer and RFC 3056 under 35 U.S.C. § 103(a).

5. In "Claim Rejections – 35 USC § 103" on page 20 of the above-identified Office Action, claim 26 was rejected as being unpatentable over Cho, Moyer and "UPnP^{TM} Secutiry Ceremonies Design Document 1.0" authored by Ellison and published by the UPnP Forum (hereinafter Ellison) under 35 U.S.C. § 103(a).

Claim 26 depends from claim 23, incorporating its recitations. Ellison was cited to read on the secure communication initiation request corresponds to a UPnP Set Session Key

(SSK) request in claim 26. However, Ellison fails to cure the deficiency of Cho and Moyer. So, based on at least one of the reasons stated above in section 1, claim 26 is patentable over Cho, Moyer and Ellison under 35 U.S.C. § 103(a).

CONCLUSION

In view of the foregoing, Applicant respectfully submits that all pending claims are in condition for allowance. Early issuance of the Notice of Allowance is respectfully requested.

Please charge any shortages and credit any overages to Deposit Account No. 500393.

Respectfully submitted,
SCHWABE, WILLIAMSON & WYATT, P.C.

Dated: December 17, 2008

/Al AuYeung/
Al AuYeung
Reg. No. 35,432

Schwabe, Williamson & Wyatt, P.C.
Pacwest Center, Suites 1600-1900
1211 SW Fifth Avenue
Portland, Oregon 97204
Telephone: 503-222-9981